BS

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/600,297	07/13/2000	JIAN HU	13267.2USWO	2701

23552 7590 01/29/2004

MERCHANT & GOULD PC
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
TRUONG, THANHNGA B	

ART UNIT	PAPER NUMBER
2135	7

DATE MAILED: 01/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/600,297	HU ET AL.	
	Examiner	Art Unit	
	Thanhnga Truong	2135	

-- The MAILING DATE of this communication appears on the cover sh et with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 July 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 July 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *4-6* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-32 are rejected under 35 U.S.C. 102(e) as being anticipated by Turk et al (US 6, 415, 271)

a. *Referring to claim 1:*

i. Turk teaches:

(1) data storage means **[i.e., referring to Figure 1, one deposit site, that is "data storage means ", having secure facilities for storage of a valuable commodity (column 4, lines 43-44)]**;

(2) a user account associated with the user **[i.e., referring to Figure 1, customer(i) 10, that is "a user account", stores gold at a storage site 12 (column 8, line 1)]**; and

(3) means for establishing a digital data transaction session in which the user is able to instruct storage or retrieval of a digital data item in association with the user's account **[i.e., referring to Figure 1, customer(i) 10 stores gold at a storage site 12 and requests the storage site to send him digital data representing certain specific values of gold, not to exceed the value of the stored gold (column 8, lines 1-3)]**;

(4) means for encoding the data item into a plurality of parts, the parts being separately stored in the storage means **[i.e., once Customer(i) receives the digital data, he can transfer all or a portion of the value of the digital**

data encoded (whereby encoding the data item into a plurality of parts is inherent) in the smartcard to another Customer(ii) 16, who also has a smartcard, for the payment of goods and/or services (arrow D). Customer(ii) then can send the digital data to the bank for storage in Customer (ii)'s account (column 8, lines 11-16)]; and

(5) means for decoding the encoded data item **[i.e., A customer, such as Customer(iii), can redeem the digital data value for gold bullion (arrow H), or if desired into a national or regional currency (such as the Euro) (column 8, lines 22-25)]**, whereby decoding the encoded data item is inherent.

b. *Referring to claim 2:*

i. Turk further teaches:

(1) wherein the data storage means comprises at least one data storage device, the parts being separately stored on the data storage device or devices **[i.e., a "storage site" as used herein is a secure facility (e.g., a vault) in which the valuable commodity (e.g., gold) is held for safekeeping. Preferably there are several storage sites for storing the commodity, that is "the parts being separately stored on the data storage device or devices" (column 5, lines 65-67)]**.

c. *Referring to claim 3:*

i. Turk further teaches:

(1) means for communication with the user **[i.e., referring to Figure 1, Customer(i) 10 stores gold at a storage site 12 and requests the storage site to send him digital data representing certain specific values of gold, not to exceed the value of the stored gold (arrow A) (column 8, lines 1-4)]**.

d. *Referring to claim 4:*

i. Turk further teaches:

(1) means for authentication of the user with the depository **[i.e., electronic cash is downloaded by the client from the bank and is held in the portable electronic device, which in one preferred embodiment, comprises a smart card (sometimes also called an "electronic purse"). The downloading occurs via a computer network that gives access, that is "for**

authentication of the user with the depository", to the client's account at his bank (column 6, lines 57-62)].

e. *Referring to claim 5:*

i. Turk further teaches:

(1) means for authentication of the depository by the user **[i.e., the users' security codes, that is "for authentication of the depository by the user", and the amount of cash to be transferred are entered into the keypad of the wallet, and the process of value transfer is triggered (column 7, lines 9-15)].**

f. *Referring to claims 6, 7, and 8:*

i. Turk further teaches:

(1) wherein the user is able to instruct retrieval of a copy of the item in said transaction session; wherein the user is able to instruct deletion of the digital data item in said transaction session; wherein the user is able to instruct an account status report in said transaction session **[i.e., in the Mondex.RTM. system, such transfers are accomplished using an intermediary electronic device known as a "wallet," into which is inserted the smartcards of both the transferring and receiving persons, wherein "the user is able to instruct retrieval of a copy of the item in said transaction session; to instruct deletion of the digital data item in said transaction session; and to instruct an account status report in said transaction session" are considered to include in this Mondex.RTM. system (column 7, line 6)].**

g. *Referring to claim 9:*

i. Turk further teaches:

(1) wherein the user's account has a data structure identifying the user and containing information identifying the data items stored therein **[i.e., the "bank" is a organization which creates account relationships with its clients and maintains information received from the storage sites regarding gold (or other commodity) held there for storage and specifically identified for use in the system. The system of the invention requires the system users to establish a fiduciary relationship with the bank. The relationship is confirmed when a system**

user either (1) stores gold with, or (2) purchases, from another person, gold already held at one or more storage sites (column 6, lines 35-43)].

h. *Referring to claim 10:*

i. Turk further teaches:

(1) wherein the information of each data item includes at least one of the type, size, time/date of submission, period of storage and pointers to the locations of the stored parts of the data item **[i.e., in the first case, the storage site verifies the receipt (in which time/date of submission is considered to include in this receipt) of the gold and provides confirmation to the system user specifying the pure weight, that is "size", and/or other physical attributes of the gold. In the second case, the storage site records the transfer of gold from one system user to the other. Then the system user informs the bank and/or storage site that he wishes to allocate some or all of his gold for use in the electronic cash system (column 6, lines 43-50)].**

i. *Referring to claim 10:*

i. Turk further teaches:

(1) wherein the means for encoding: a) divides the data item into a multiple of q K-tuples, denoted as $X_i = (x_{i1}, x_{i2} \ldots x_{iK})$, I = 1 to q, where x is a symbol over $GF(2^m)$ with m being a positive integer; b) for i = I to q, encodes Xi into a codeword $Y_i = (y_{i1}, Y_{i2} \ldots y_{jN})$ using an (N, K) error-control code C, where Y_{ij}, is a symbol over $GF(2^m)$; c) rearranges Y_j, for i = 1 to q, into q-tuples Z, $(y_{1j}\ y_{2j} \ldots y_{qj})$, for j = 1 to N; and d) stores the Z_j, for j = 1 to N, as said parts **[i.e., in one such method known as the RSA algorithm, encryption and decryption are accomplished by two mathematical equations which are related as inverses of each other. These equations are the private key, used by the issuing financial institution to digitally sign, or certify, a note, and the related public key, used by the recipient to determine and verify the existence of a valid signature on the note, whereby the above claimed limitation is considered to include in this RSA algorithm (column 5, lines 30-37)].**

j. *Referring to claim 12:*

i. Turk further teaches:

(1) wherein the means for decoding: a) on inputting a data item identity, for j = 1 to N, reads $Z'_j = (y'_{1j}\ y'_{2j} \ldots y'_{qj},)$ from the locations where Z_j was stored, where Z_j, j = 1 to N, are the parts of the data item as identified; b) rearranges Z'_j, for j = 1 to N, into N-tuples $Y'_i = (y'_{i1}, Y'_{i2} \ldots y'_{iN})$, for i = 1 to q; c) decodes Y'i using an error- and -erasu re-co rrec ti on decoder of the (N, K) code C to obtain $X'j = (x'_{j1}, X'_{i2} \ldots x'_{iK})$, for i = 1 to q; and d) concatenates X'_j, for i = 1 to q to form the data item **[i.e., in one such method known as the RSA algorithm, encryption and decryption are accomplished by two mathematical equations which are related as inverses of each other. These equations are the private key, used by the issuing financial institution to digitally sign, or certify, a note, and the related public key, used by the recipient to determine and verify the existence of a valid signature on the note, whereby the above claimed limitation is considered to include in this RSA algorithm (column 5, lines 30-37)].**

k. *Referring to claims 13, 15, and 16:*

i. These claims have limitations that is similar to those of claim 12, thus they are rejected with the same rationale applied against claim 12 above.

l. *Referring to claim 14:*

i. This claim has limitations that is similar to those of claim 11, thus it is rejected with the same rationale applied against claim 11 above.

m. *Referring to claim 17:*

i. Turk further teaches:

(1) means for encryption of the data item **[i.e., in the context of encrypted communications the public key is used to encrypt electronic data which can only be decrypted using the matched private key (column 5, lines 15-18)];**

n. *Referring to claim 18:*

i. Turk further teaches:

(1) wherein the user is able to instruct encryption, prior to encoding, of the data item to be stored during the transaction session **[i.e.,**

these equations are the private key, used by the issuing financial institution to digitally sign, or certify, a note, and the related public key, used by the recipient, that is "the user", to determine, that is "to instruct encryption", and verify the existence of a valid signature on the note (column 5, lines 33-37)].

o. *Referring to claim 19:*

i. Turk further teaches:

(1) wherein the information of each data item includes an indication of whether or not the item is encrypted and a pointer to a decryption key **[i.e., the "bank" is a organization which creates account relationships with its clients and maintains information received from the storage sites regarding gold (or other commodity) held there for storage and specifically identified for use in the system (column 6, lines 35-39). In addition, public key encryption methods have been developed for use in electronic cash. Furthermore, in the context of encrypted communications, the private key is used to decrypt electronic data encrypted with the corresponding public key (column 5, lines 21-30)].**

p. *Referring to claim 20:*

i. This claim has limitations that is similar to those of claim 19, thus it is rejected with the same rationale applied against claim 19 above.

q. *Referring to claims 21 and 24:*

i. These claims have limitations that is similar to those of claim 18, thus they are rejected with the same rationale applied against claim 18 above.

r. *Referring to claims 22 and 23:*

i. Turk further teaches:

(1) wherein the means for checking decodes, checks and reencodes the data item at intervals; and wherein the intervals are of fixed or variable period. **[i.e., the RSA algorithm, that is "for checking decodes, checks and reencodes the data item at intervals" (column 5, line 31)].**

s. *Referring to claim 25:*

i. Turk further teaches:

(1) wherein the integrity check comprises a digital signature **[i.e., "Private key" is a mathematical key which is kept private to the owner and which is used to create digital signatures. In addition, A digital signature is an application of public key cryptography in that the key used to verify, that is "the integrity check", the signature is different from the key used to sign the signature (column 5, lines 19-29)].**

t. *Referring to claim 26:*

i. This claim has limitations that is similar to those of claim 5, thus it is rejected with the same rationale applied against claim 5 above.

u. *Referring to claim 27:*

i. Turk further teaches:

(1) wherein communication with the user during the transaction session is by means of a plurality of messages each associated with a transaction to be performed **[i.e., referring to Figure 1, "a plurality of messages each associated with a transaction to be performed" is considered to be sent to and from the storage site and the customers].**

v. *Referring to claims 28 and 29:*

i. These claims have limitations that is similar to those of claim 27, thus they are rejected with the same rationale applied against claim 27 above.

w. *Referring to claim 31:*

i. This claim has limitations that is similar to those of claims 1 and 4, thus it is rejected with the same rationale applied against claims 1 and 4 above.

x. *Referring to claim 32:*

i. Turk further teaches:

(1) receiving an instruction to retrieve a stored and encoded data item, decoding the data item and sending the data item to the user **[i.e., referring to Figure 1, the "bank" is a organization which creates account**

relationships with its clients and maintains information received from the storage sites regarding gold (or other commodity) held there for storage and specifically identified for use in the system (column 6, lines 35-39), wherein "receiving an instruction to retrieve a stored and encoded data item, decoding the data item and sending the data item to the user" is also considered to include in this "bank"].

3. Claims 33-35 are rejected under 35 U.S.C. 102(e) as being anticipated by Carroll (US 6,105, 131)

a. *Referring to claim 33:*

i. Carroll teaches:

(1) a data depository in which digital data may be stored electronically **[i.e., referring to Figure 1, The secure server 12 includes a vault deposit server ("VDSI") 20 connected to a certification management system ("CMS") 24 and optionally a directory services 22 (column 4, lines 14-16)];**

(2) providing for registration of users of the data depository, each user having an account with the depository **[i.e., referring to Figure 1, a registration authority terminal 16 can be connected to the computer network 14, that is for "providing for registration of users of the data depository", and each user can have a personal vault, that is "an account with the depository", as shown in Figure 2];**

(3) in response to a request from a user, opening a transaction session with the user in which the user and the depository authenticate each other and performing a transaction instructed by the user in respect of a digital data item, the transaction being selected by the user from a plurality of available transactions including storage of the item in or retrieval of the item from the depository **[i.e., in Figure 4B, a new account request form illustrates a set of fields. The fields may include user specific information such as name, address, and telephone number, transaction information such as account type, fund transfer, and deposit method, and terminal information such as the storage location of the certificate. The session can be secured by using SSL communication. Secure session are**

indicated by an unbroken arrow in the lower left hand corner of the screen (column 7, lines 1-8)].

b. *Referring to claim 34:*

i. Carroll further teaches:

(1) in which storage of the item includes encoding the item into a plurality of parts and storing the parts separately in the depository **[i.e., a system including a secure server and processes enabling operating system integration through virtual logon and user data encrypted in "personal vaults", wherein "encoding the item into a plurality of parts and storing the parts separately in the depository" is considered to include in this "personal vaults" (column 1, lines 54-57)].**

c. *Referring to claim 35:*

i. Carroll further teaches:

(1) the step of checking, at intervals, the integrity of data items stored in the depository **[i.e., referring to Figure 1, "the step of checking, at intervals, the integrity of data items stored in the depository" is considered to include in the secure server 12].**

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Patel et al (US 6, 438, 690 B1) discloses a secure end-to-end communications system includes a vault controller based registration application for managing the issuance and administration of digital certificates for use in conducting electronic commerce in the system (see abstract).

b. Cohen (US 6, 356, 941 B1) discloses the network vault is similar to a physical safe, in that substantially any type of information can be stored in the network vault, and in that the user need only place the information inside the network vault for the information to be secured (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT
January 14, 2004

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100